OAuth 2.0 and OpenID Connect in the Swiss edu-ID

Rolf Brugger
rolf.brugger@switch.ch

Swiss edu-ID Update, 13. August 2015

Motivation to consider OAuth 2.0 and OpenID Connect

- Enable native mobile applications and non-web resources
  - Shibboleth/SAML is a web browser based technology
- Provide more developer-friendly environment
  - Shibboleth setup and configuration is complex
  - But complexity of scalable OIDC federation unknown

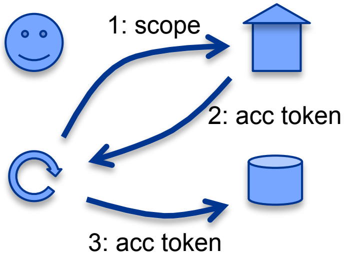
OAuth 2.0

- Framework for authorization protocols
  - Avoid password proliferation
  - Protect APIs
  - Mobile access to server systems
  - User authentication
- Specifies a set of message flows
- Based on http and JSON
- Specification finalized: October 2012 (RFC6749)

OpenID Connect

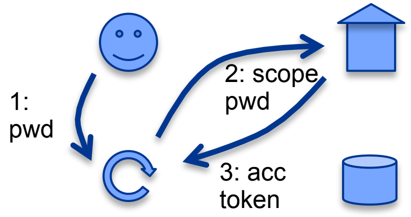
- Provides identity services: adds user attributes (ID Token)
  - User ID, profile data, authentication meta information
- Based on OAuth 2.0
- Scalable security model (ISO/IEC29115 LoA1…4)
- Base specification finalized: February 2014
  - Missing application profiles like interoperable attribute specifications

OAuth 2.0 Flows

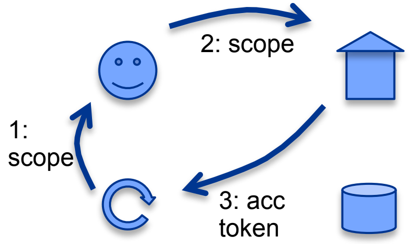


OAuth 2.0 usage scenarios (flows)

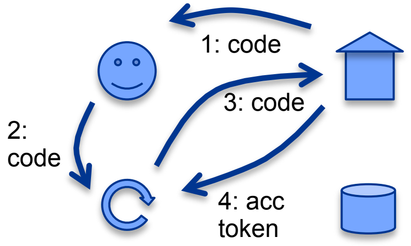
- Service-service communication:
  client credential flow
  - Without involving a user



- Trusted clients:
  resource owner password credential flow
  - Client sees password



- Untrusted clients: *implicit flow*
  - Password not revealed to client



- Client runs on server: *authorization code flow*
  - Token stored on server side (ORCID case)

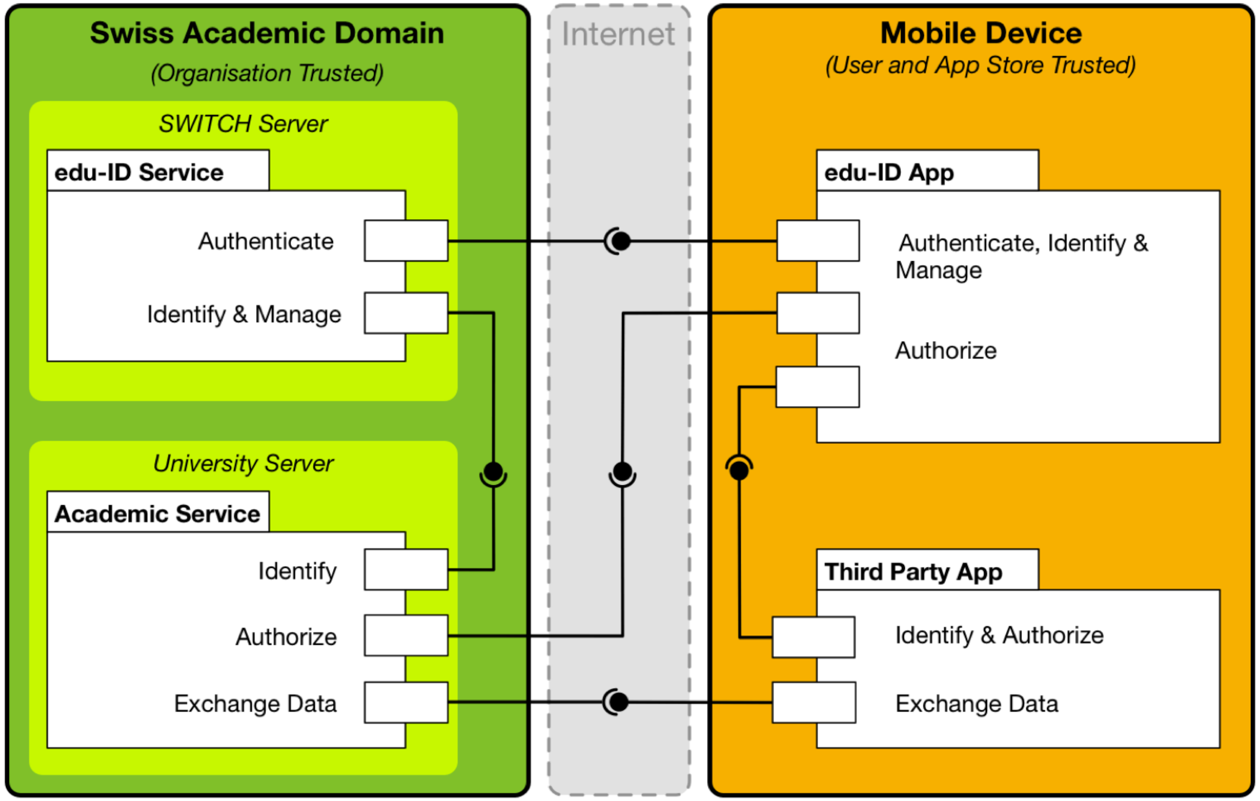
Differences between SAML and OIDC

	SAML/shibboleth	OpenID Connect
Federation support	yes	no (no federation metadata)
Developer friendliness	Not reqired	Relying party libraries for various languages
Setup and operation of service	Shibboleth software suite, updates, certificates	OIDC library installation
Non-web / mobile application support	no	yes
Access delegation	difficult (ECP)	yes, including user-initiated token revocation

No fundamental differences: attribute provider, user consent, IdP middleware/server, application registry

Pilot Project: Mobile App

- One single authentication app authorizes many local third party apps
- Supports native apps and hybrid mobile apps
- Proof-of-concept:
  - Integrate mobile apps and LMS
  - Integration with Swiss edu-ID



Other prospective Pilot Projects

- Event registration at FHNW
  - IT services provide registration API (exposed to the public)
  - Departments implement customized registration forms using the API
  - Users allow registration forms to access the institutional person information system (access delegation)

Support for OAuth and OIDC in Swiss edu-ID

Option: Extend Shibboleth

- Shibboleth 3.0 IdP has modular architecture
- OIDC and OAuth are on Shibboleth roadmap with status “under discussion”
- Pilots are possible with 3rd party OAuth suites outside of shibboleth

Option: alternative AM product OpenAM

- OpenAM fully supports OAuth 2.0 and OIDC
- Proof-of-concept (July 2015): OpenAM can be made compatible to the SWITCHaai federation

Call for Participation

- Tell us your use-cases
- Let’s start pilot projects together